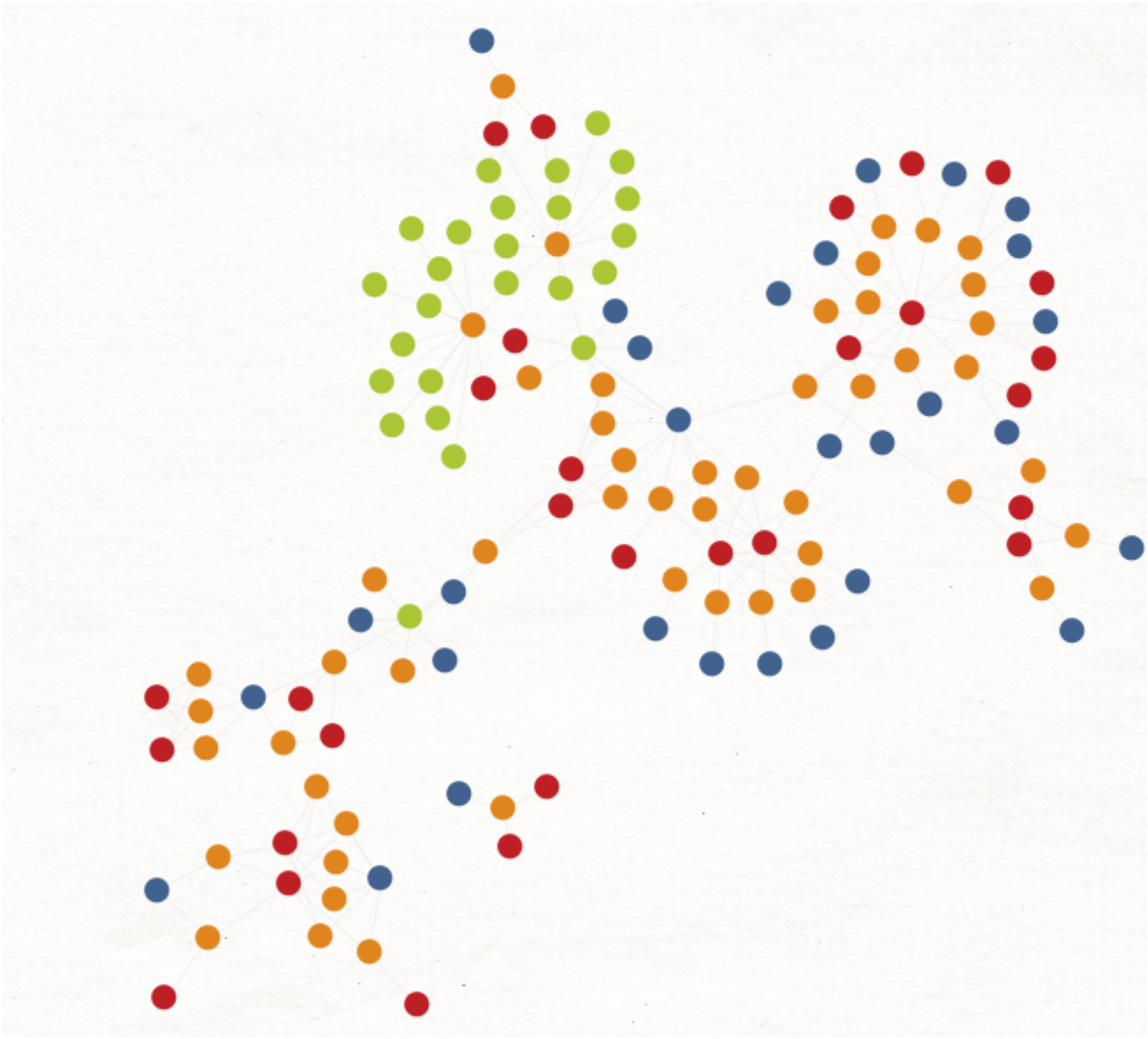
00. Security Researchers Targeted in a Spear Phishing Campaign - An Analysis



We've become recently aware of a targeted spear phishing and actual client-side exploits dropping malicious campaign targeting legitimate security researchers by approaching them personally or using social media in an attempt to entice them into verifying the validity of a supposedly newly discovered and recently launched Zero Day flaw which in reality once executed drops malicious software on the hosts of the affected researchers and we've decided to research even further and offer practical and relevant including actionable intelligence on the campaign's infrastructure for the purpose of assisting fellow researchers and the industry on its way to track down and monitor the campaign.

In this analysis we'll take a closer look at the campaign and provide actionable intelligence on the infrastructure behind it and discuss in-depth the TTPs (Tactics Techniques and Procedures) of the cybercriminals behind it.

Screenshot of the fake security company Web site generated by WhoisXML API's Screenshot Generation Service

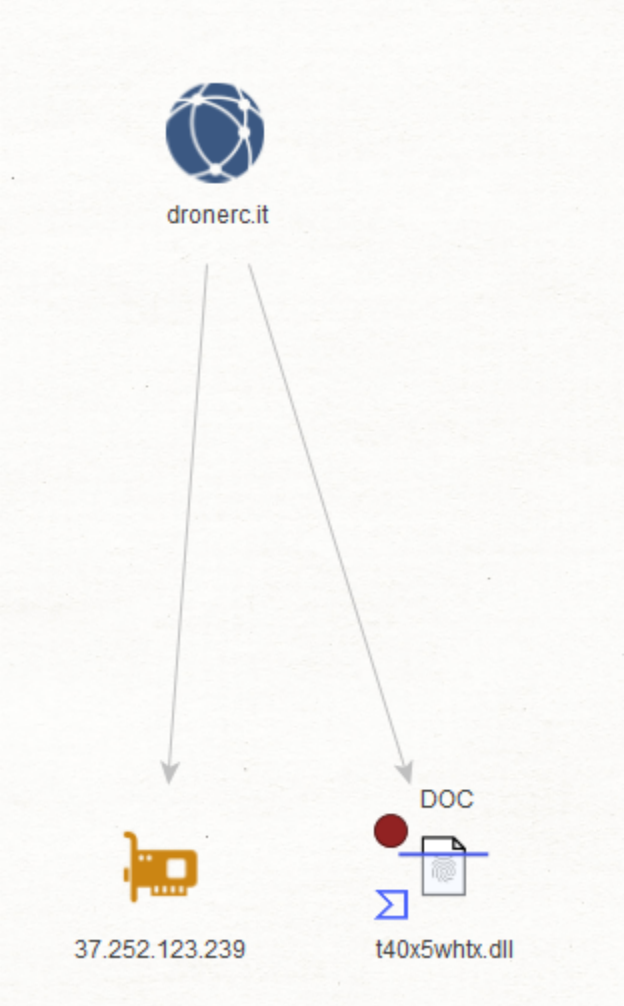
Official rogue security research Web site's responding IPs:

- hxxp://193.29.57.231
- hxxp://68.65.122.10

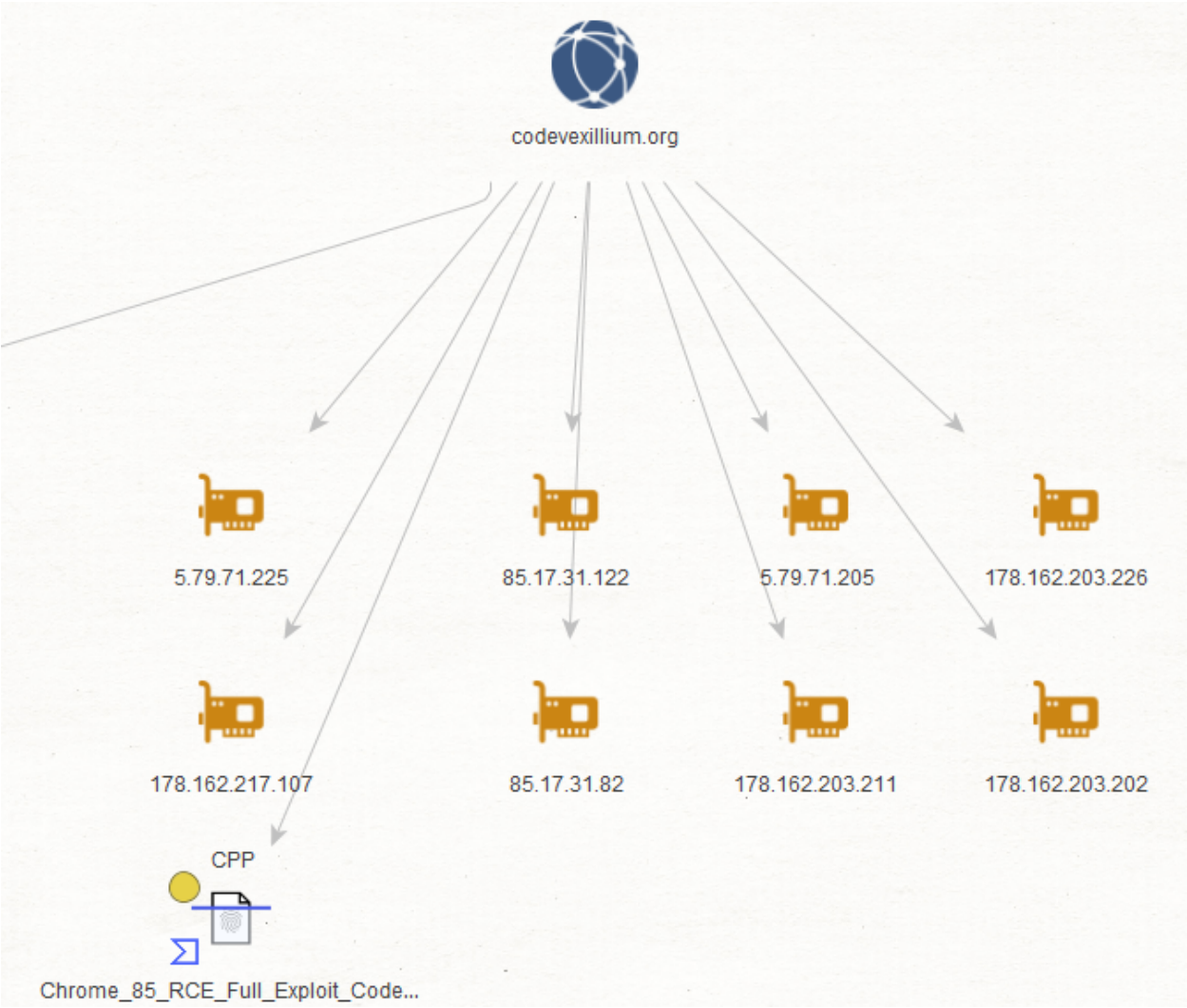
Sample malicious domains including C&C phone back locations known to have participated in the campaign:

- angeldonationblog.com
- codevexillium.org
- investbooking.de
- krakenfolio.com
- opsonew3org.sg
- transferwiser.io
- Transplugin.io
- trophylab.com
- colasprint.com
- dronerc.it
- edujikim.com
- fabioluciani.com
- bestwing.org
- codebiogblog.com
- coldpacific.com
- cutesaucepuppy.com
- devguardmap.org
- hireproplus.com
- hotelboard.org
- mediterraneanroom.org
- redeastbay.com
- regclassboard.com

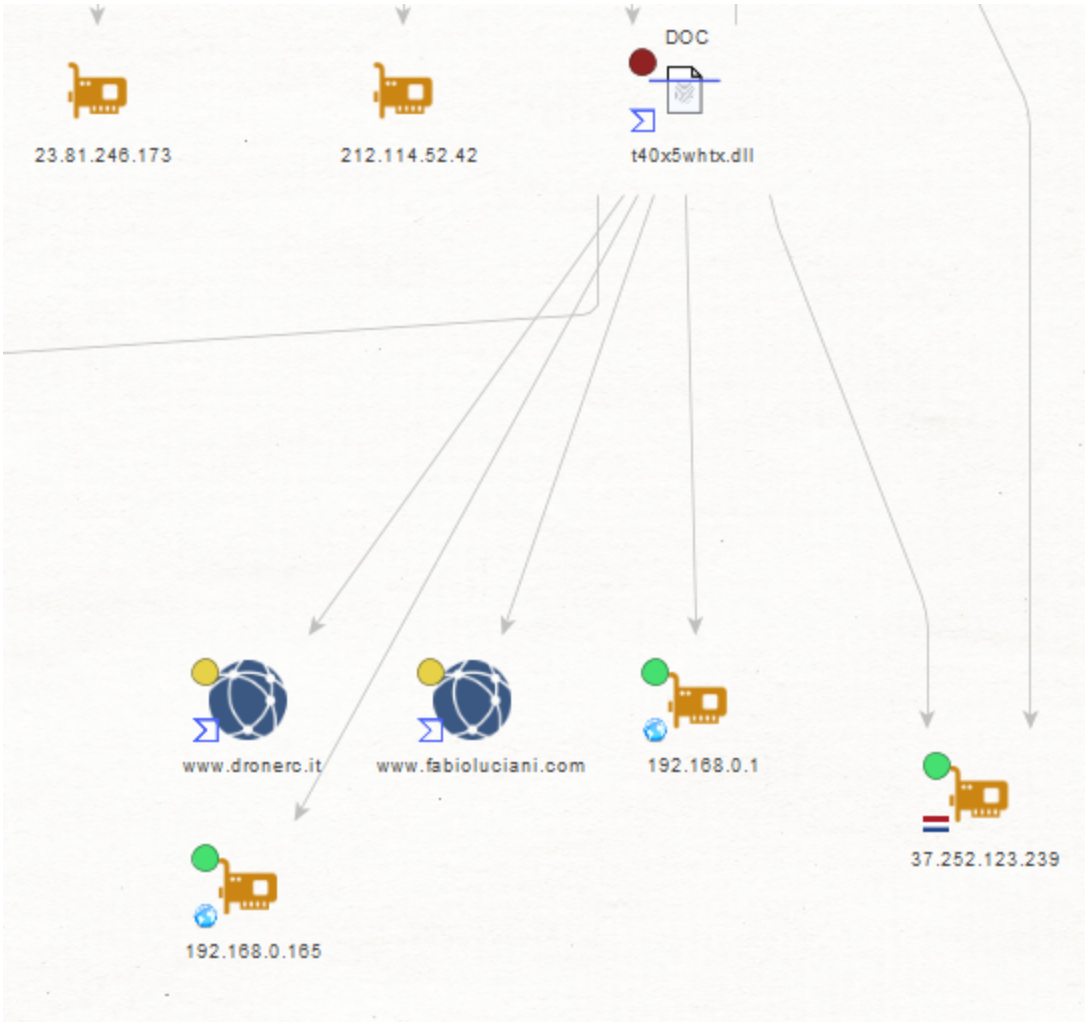
- securielite.com
- spotchannel02.com
- wileprefgurad.net



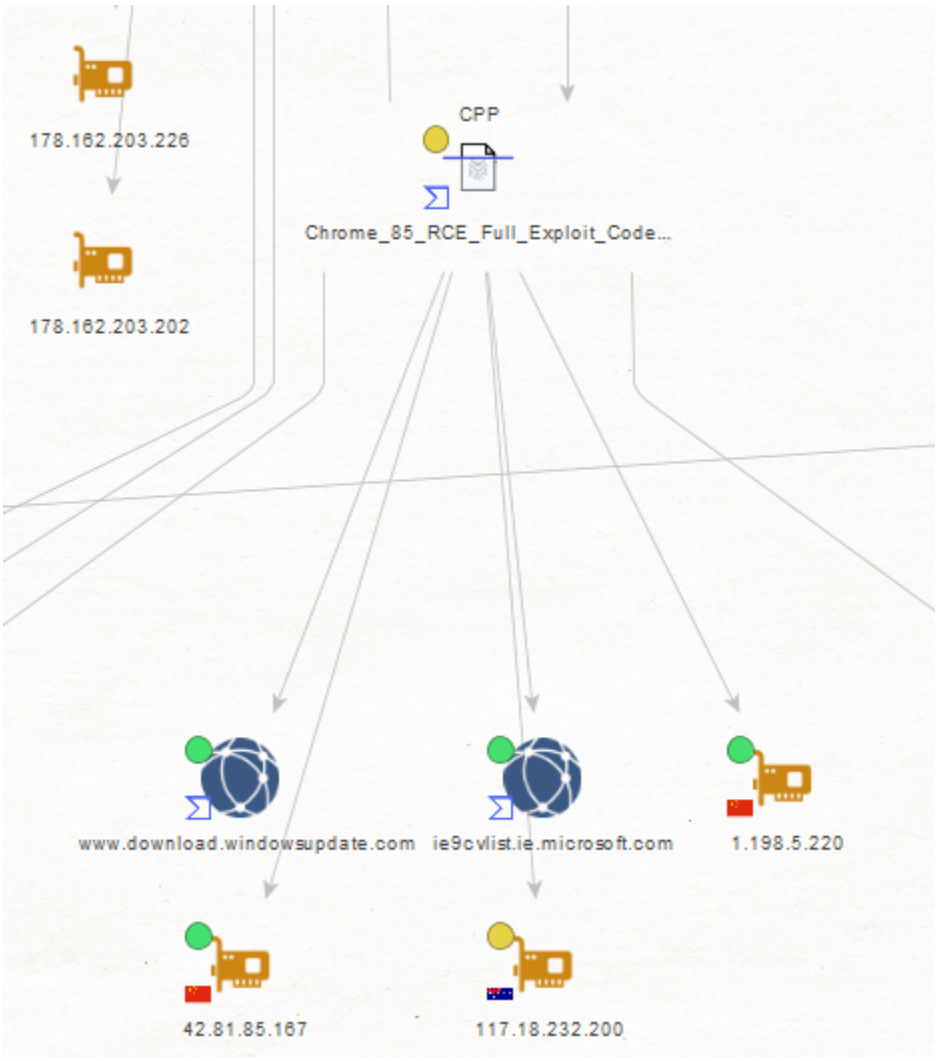
Sample Screenshot of a sample malicious MD5 that's known to have phoned back to one of the C&C infrastructure domains



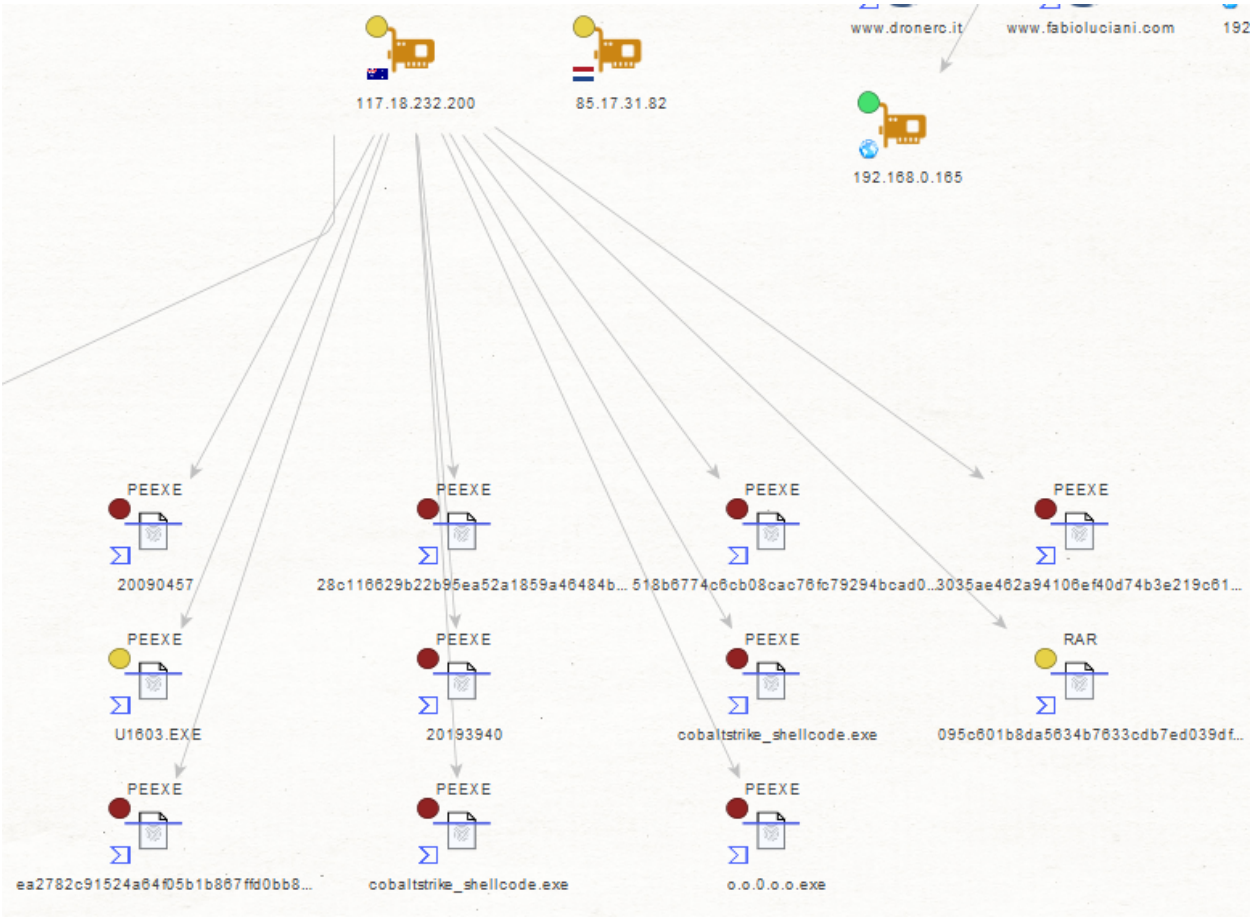
Sample Screenshot of a sample malicious MD5 that's known to have phoned back to one of the C&C infrastructure domains



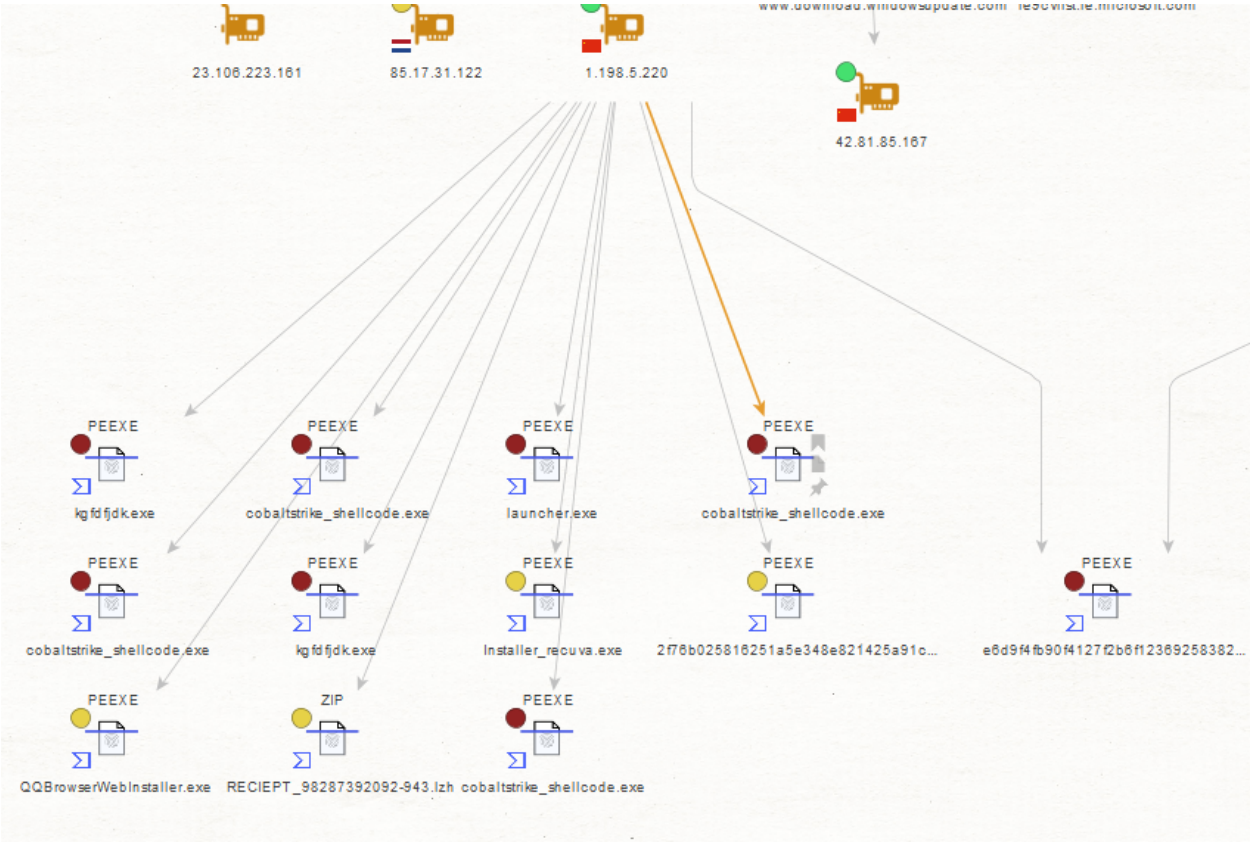
Sample Screenshot of a sample malicious MD5 that's known to have phoned back to one of the C&C infrastructure domains



Sample Screenshot of a sample malicious MD5 that's known to have phoned back to one of the C&C infrastructure domains



Sample Screenshot of a sample malicious MD5 that's known to have phoned back to one of the C&C infrastructure domains



Sample Screenshot of a sample malicious MD5 that's known to have phoned back to one of the C&C infrastructure domains

Sample malicious and rogue IPs known to have responded to the same malicious and fraudulent domains part of the campaign:

23.106.223.161

23.106.122.108

42.81.85.167

117.18.232.200

23.106.122.133

1.198.5.220

45.147.228.158

108.62.118.136

23.106.123.191

45.153.240.142

118.107.163.120

61.110.214.203

14.0.92.60

45.147.231.213

52.231.31.103

162.255.119.131

61.110.215.123

175.125.95.173

103.253.40.225

23.81.246.173

108.177.235.178

192.168.0.165

192.168.0.1

62.149.128.157

188.165.161.229

62.149.128.154

193.70.64.169

23.106.215.130

212.114.52.42

178.162.203.202

85.17.31.82

178.162.203.211

178.162.203.226

178.162.217.107

85.17.31.122

5.79.71.205

5.79.71.225

193.29.57.231

50.192.28.29

198.54.117.244

23.106.215.15

210.219.173.87

211.233.13.82

23.236.62.147

198.54.126.85

23.106.122.88

62.149.128.151

212.114.52.57

45.147.230.201

37.252.123.239

54.227.98.220

Related malicious MD5s known to have phoned back to the same malicious infrastructure or have participated in the campaign:

6f0472278d265d581aa291792a34c7fcbdce8e95b94c0e45e52c23c7c4a2e057

ec3125384833c72867d16a1a6f5b833d8aede46a560a605fd20ec1f63805acfc

8184b3d09c1fb015c7829efad7310eefc8da7804d578ccb10f15301cbb957e6a

e4030770c5d6671c5e4b57cb21e99e22407b25e0077f5ddca494561c6c3703bc

668493ea5a263986d42f696f809f43e9cee7b655192248d1863c765e259b64a7

a4d413cab72b17f19a26ea2281d6c896aabd25e4e63dc0fc826ec2b1f8c2b46c

5dc0eb68a99e4b945641b33fcca2c4ad3b3f67179006d2a974a605ced2483894

cd16cb61dc5eac8e5c00a6ce22a1958fa9ba4da668c3b9578cad45a0ef7ca332

8b1cdfb26d6f128b147da61decdbc3e9e6416c65b8c70ec0a6d028cb7b2454be

aba56831029c8f89b3aaf697959c01bfcf546969ff79c6ee848e275b84214393

4ff241b82b67e56611ac7a768ddb0613af9f6d55afa4034246a5a3ed4a3f157e

e6d9f4fb90f4127f2b6f1236925838270725293 91ae2eb0bf9f83711525c5e21

8e896c58a8d54b5773782a8dd93529c842ed27f6a9dbbe32afdd0ea98b58dbd1

0e8ada682fc995c7667ef30fd6f00fccb3cfceded919ff535bd4d954ff3140b8

99d4884921df6b98cf3ca2aa131b4ca1aad7961ad5b0552167de684e0333df89

bc0c5d8bf4067320024613792712 1b738190043a5ded8c13cfb0ed92340dd5eb

066623257995233ed8833d2681ce23032067b23422053ac10c9f7ff6c2a56e9f

9ffb8ce09d03702cce10c73126aa71d87f82ed951001c75d21c29633b7c8879f

b3880aa40a577e8f23091288864718ddfacd8789a927730eba67e65bc3da224f

a882cea7addb1d379c8b55148b9e51646983620b2fb9366573a113c76a347672

095c601b8da5634b7633cdb7ed039dfb5cd4eb19e076c119d0a0abb84bec90e7

a23c44799e8274270cd2664ac9a3c5abe17461f4f13e4625e0886c12df1128a3

5c6f22baab3c51231c211e25428f3b33f30800fd97e7140bd6b0bc4fee82bcab

We'll continue monitoring the campaign using WhoisXML API's infrastructure for domain and registrant monitor and will issue an update as soon as new developments take place.